

Klären der Regelaktionen der Firepower Threat Defense-Richtlinien zur Zugriffskontrolle

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Bereitstellung von ACP](#)

[Konfigurieren](#)

[Verfügbare AKP-Aktionen](#)

[Interaktion zwischen ACP und Prefilter-Richtlinie](#)

[AKP-Blockaktion](#)

[Szenario 1. Früher LINA-Ausfall](#)

[Szenario 2. Fallenlassen aufgrund von Snort Verdict](#)

[ACP-Block mit Rücksetzaktion](#)

[ACP-Zulassungsaktion](#)

[Szenario 1. ACP-Zulassungsaktion \(L3/L4-Bedingungen\)](#)

[Szenario 2. ACP-Zulassungsaktion \(L3-7-Bedingungen\)](#)

[Szenario 3. Snort Fast-Forward-Verdict mit Allow](#)

[AKP-Treuhandaktion](#)

[Szenario 1. ACP Trust Action](#)

[Szenario 2. ACP Trust Action \(ohne SI, QoS und Identitätsrichtlinie\)](#)

[Sperrern von Richtlinien vorfiltern](#)

[Vorfilter-Policy Fastpath-Aktion](#)

[Fastpath-Aktion der Vorfilterrichtlinie \(Inline-Set\)](#)

[Prefilter Policy FastPath Action \(Inline-Set mit Tap\)](#)

[Aktion zur Richtlinienanalyse vorfiltern](#)

[Szenario 1. Vorfilter Analyse mit ACP-Blockregel](#)

[Szenario 2. Vorfilter Analyse mit ACP-Zulassungsregel](#)

[Szenario 3. Vorfilter Analyse mit ACP Trust Rule](#)

[Szenario 4. Vorfilter Analyse mit ACP Trust Rule](#)

[AKP-Überwachungsaktion](#)

[Interaktive AKP-Blockaktion](#)

[Interaktiver AKP-Block mit Rücksetzaktion](#)

[Sekundäre FTD-Verbindungen und Pinholes](#)

[FTD-Richtlinien](#)

[Zusammenfassung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die verschiedenen verfügbaren Aktionen der Zugriffskontrollrichtlinie (Access Control Policy, ACP) und der Vorfilterrichtlinie von Firepower Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Flow Offload
- Paketerfassung auf Firepower Threat Defense-Appliances
- Packet Tracer und Erfassung mit Trace-Option auf FTD-Appliances

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Firepower 4110 Threat Defense Version 6.4.0 (Build 113) und 6.6.0 (Build 90)
- FirePOWER Management Center (FMC) Version 6.4.0 (Build 113) und 6.6.0 (Build 90)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

- ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5516-X
- ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X
- FPR1000, FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-basiertes virtuelles System (KVM)
- Integrated Service Router (ISR)-Router-Modul
- FTD-Softwareversion 6.1.x und höher

Anmerkung: Flow Offload wird nur auf nativen Instanzen der ASA- und FTD-Anwendungen sowie auf den Plattformen FPR4100 und FPR9300 unterstützt. FTD-Containerinstanzen unterstützen kein Flow Offload.

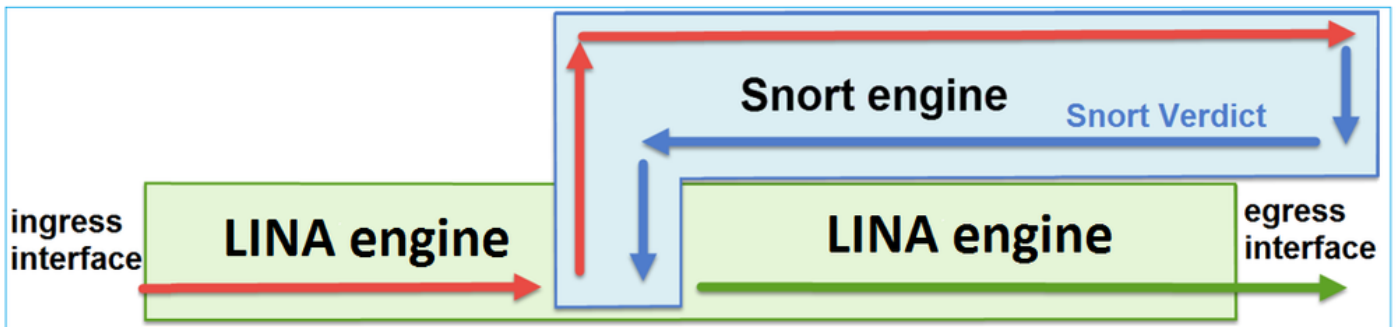
Hintergrundinformationen

Die Hintergrundoperation jeder Aktion wird zusammen mit ihrer Interaktion mit anderen Funktionen wie Flow Offload und Protokollen, die sekundäre Verbindungen öffnen, untersucht.

FTD ist ein vereinheitlichtes Software-Image, das aus zwei Hauptkomponenten besteht:

- LINA-Motor
- Snort-Engine

Diese Abbildung zeigt, wie die beiden Engines interagieren:



- Ein Paket gelangt an die Eingangsschnittstelle und wird von der LINA-Engine verarbeitet.
- Wenn dies nach der FTD-Richtlinie erforderlich ist, wird das Paket von der Snort-Engine geprüft.
- Die Snort-Engine gibt ein Urteil (Erlaubnisliste oder Sperrliste) für das Paket zurück
- Die LINA-Engine verwirft oder leitet das Paket basierend auf dem Urteil von Snort weiter.

Bereitstellung von ACP

Die FTD-Richtlinie wird auf dem FMC konfiguriert, wenn die externe (Remote-) Verwaltung verwendet wird, oder auf dem Firepower Device Manager (FDM), wenn die lokale Verwaltung verwendet wird. In beiden Szenarien wird der ACP wie folgt bereitgestellt:

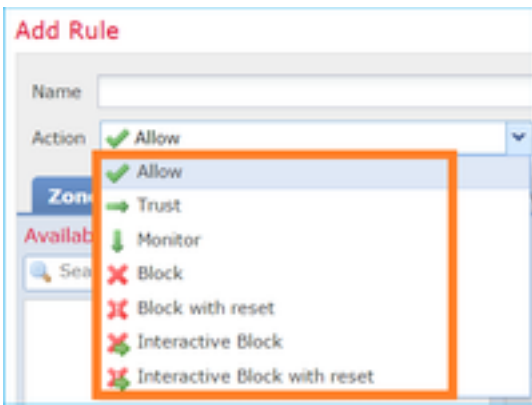
- eine globale Zugriffskontrollliste mit dem Namen CSM_FW_ACL_ für die FTD LINA-Engine
- Zugriffskontrollregeln in der Datei /ngfw/var/sf/detection_engines/<UUID>/ngfw.rules auf die FTD Snort Engine

Konfigurieren

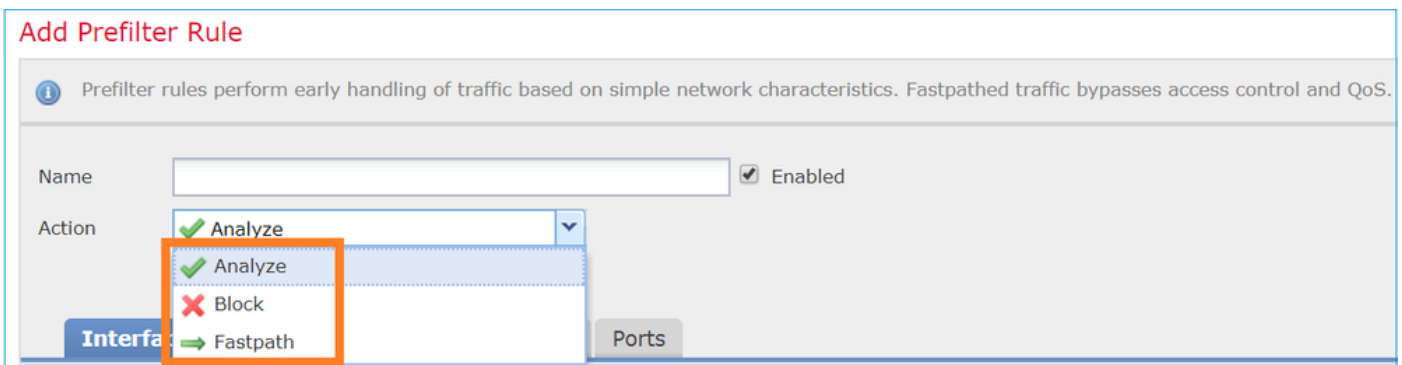
Verfügbare AKP-Aktionen

Der FTD ACP enthält eine oder mehrere Regeln, und jede Regel kann eine dieser Aktionen ausführen. Wie in der Abbildung dargestellt,

- Allow
- Trust
- Monitor
- Block
- Block with reset
- Interactive Block
- Interactive Block with reset



Ebenso kann eine Vorfilterrichtlinie eine oder mehrere Regeln enthalten, und die möglichen Aktionen werden im Bild angezeigt:



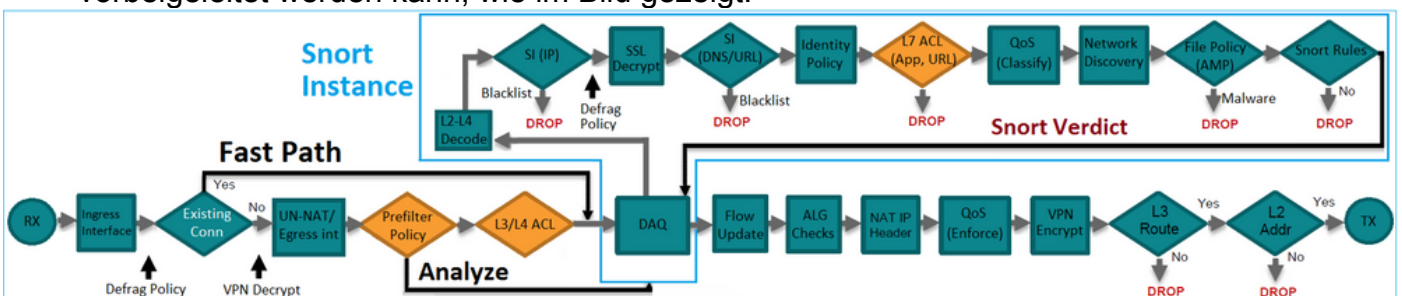
Interaktion zwischen ACP und Prefilter-Richtlinie

Die Prefilter-Richtlinie wurde in Version 6.1 eingeführt und erfüllt zwei Hauptaufgaben:

1. Es ermöglicht die Überprüfung des getunnelten Datenverkehrs, wobei die FTD LINA-Engine den äußeren IP-Header überprüft, während die Snort-Engine den inneren IP-Header überprüft. Genauer gesagt, im Fall von getunneltem Datenverkehr (z. B. GRE) werden die Regeln in der Prefilter-Richtlinie immer auf die **outer headers**, während die Regeln in den AKP-Staaten immer für die internen Sitzungen gelten (**inner headers**). Der getunnelte Datenverkehr bezieht sich auf folgende Protokolle:

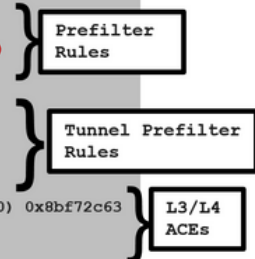
- GRE
- IP-in-IP
- IPv6-in-IP
- Teredo-Port 3544

2. Es bietet Early Access Control (EAC), mit dem der Fluss vollständig an der Snort-Engine vorbeigeleitet werden kann, wie im Bild gezeigt.



Die Vorfilterregeln werden auf FTD als L3/L4-Zugriffskontrollelemente (Access Control Elements, ACEs) bereitgestellt und gehen den konfigurierten L3/L4-ACEs wie in der Abbildung dargestellt voraus:

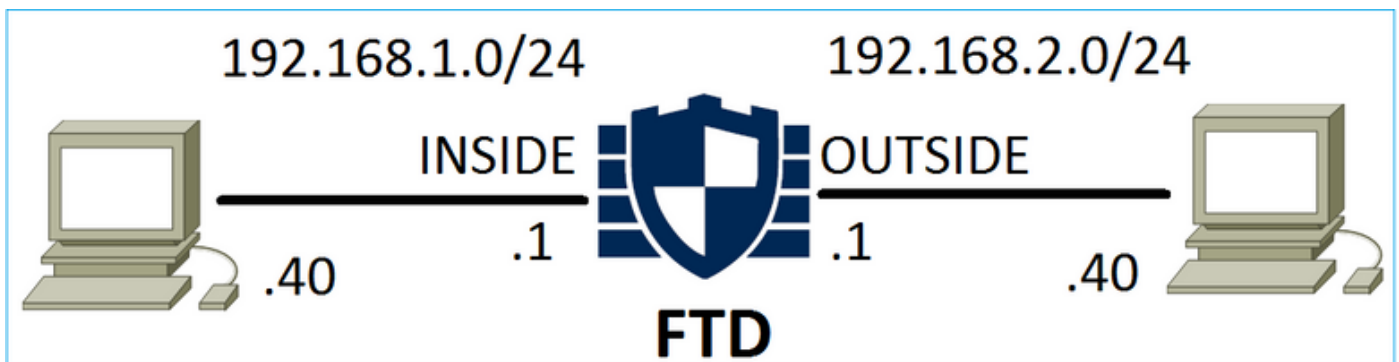
```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log both (hitcnt=0)
access-list CSM_FW_ACL_ line 4 remark rule-id 268434456: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268434456: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id 268434456 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268434456 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268434456 (hitcnt=2) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any any eq 3544 rule-id 268434456 (hitcnt=0) 0xcf6309bc
access-list CSM_FW_ACL_ line 10 remark rule-id 268434445: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ line 12 advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start (hitcnt=0) 0x8bf72c63
access-list CSM_FW_ACL_ line 14 remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 15 advanced permit ip any any rule-id 268434434 (hitcnt=410) 0xa1d3780e
```



Anmerkung: Prefilter v/s ACP-Regeln = die erste Übereinstimmung wird angewendet.

AKP-Blockaktion

Beachten Sie die in diesem Bild gezeigte Topologie:



Szenario 1. Früher LINA-Ausfall

Der ACP enthält eine Blockregel, die eine L4-Bedingung verwendet (Ziel-Port TCP 80), wie in der Abbildung dargestellt:

Access Control > Access Control													
Network Discovery Application Detectors Correlation Actions													
ACP1													
Enter Description													
Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None													
Rules Security Intelligence HTTP Responses Advanced													
Filter by Device Show Rule Conflicts Add Category Add Rule Search Rule													
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	Block

Die in Snort bereitgestellte Richtlinie:

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

Die bereitgestellte Richtlinie in LINA. Beachten Sie, dass die Regel verschoben wird als deny aktion:

```
firepower# show access-list
```

```
...  
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1  
access-list CSM_FW_ACL_ line 10 advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www  
rule-id 268435461 event-log flow-start (hitcnt=0) 0x6149c43c
```

Verhalten überprüfen:

Wenn Host-A (192.168.1.40) versucht, eine HTTP-Sitzung zu Host-B (192.168.2.40) zu öffnen, werden die TCP-Synchronisierungspakete (SYN) von der FTD LINA-Engine verworfen und erreichen die Snort Engine oder das Ziel:

```
firepower# show capture
```

```
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -  
430 bytes]  
  match ip host 192.168.1.40 any  
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -  
0 bytes]  
  match ip host 192.168.1.40 any
```

```
firepower# show capture CAPI
```

```
  1: 11:08:09.672801 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920  
<mss 1460,sackOK,timestamp 4060517 0>  
  2: 11:08:12.672435 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920  
<mss 1460,sackOK,timestamp 4063517 0>  
  3: 11:08:18.672847 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920  
<mss 1460,sackOK,timestamp 4069517 0>  
  4: 11:08:30.673610 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920  
<mss 1460,sackOK,timestamp 4081517 0>
```

```
firepower# show capture CAPI packet-number 1 trace
```

```
  1: 11:08:09.672801 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920  
<mss 1460,sackOK,timestamp 4060517 0>  
...
```

```
Phase: 4
```

```
Type: ACCESS-LIST
```

```
Subtype: log
```

```
Result: DROP
```

```
Config:
```

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id  
268435461 event-log flow-start
```

```
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
```

```
access-list CSM_FW_ACL_ remark rule-id 268435461: L4 RULE: Rule1
```

```
Additional Information:
```

```
<- No Additional Information = No Snort Inspection
```

```
Result:
```

```
input-interface: INSIDE
```

```
input-status: up
```

```
input-line-status: up
```

```
output-interface: OUTSIDE
```

```
output-status: up
```

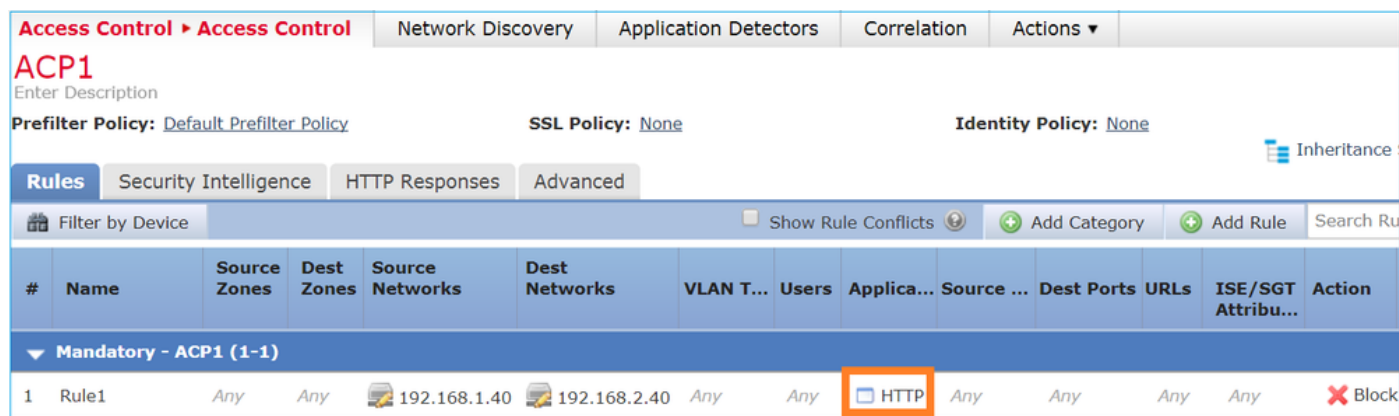
```
output-line-status: up
```

```
Action: drop
```

```
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Szenario 2. Fallenlassen aufgrund von Snort Verdict

Der ACP enthält eine Block-Regel, die eine L7-Bedingung (Application HTTP) verwendet, wie im Bild gezeigt:



#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	HTTP	Any	Any	Any	Any	Block

Die in Snort bereitgestellte Richtlinie:

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any (appid 676:1)
```

Appid 676:1 = HTTP

Die bereitgestellte Richtlinie in LINA.

Anmerkung: Die Regel wird als **permit**-Aktion, da LINA nicht feststellen kann, dass die Sitzung HTTP verwendet. Auf FTD befindet sich der Mechanismus zur Anwendungserkennung in der Snort-Engine.

```
firepower# show access-list
```

```
...  
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1  
access-list CSM_FW_ACL_ line 10 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id  
268435461 (hitcnt=0) 0xb788b786
```

Für eine Blockregel, die Folgendes verwendet: **Application** als Bedingung zeigt die Ablaufverfolgung eines realen Pakets an, dass die Sitzung von der LINA aufgrund des Snort-Engine-Urteils verworfen wird.

Anmerkung: Damit die Snort-Engine die Anwendung bestimmt, muss sie einige Pakete überprüfen (in der Regel 3-10, je nach Anwendungsdecoder). So werden ein paar Pakete durch die FTD zugelassen und gelangen an das Ziel. Die zulässigen Pakete unterliegen weiterhin der Prüfung der Angriffsrichtlinie, die auf dem **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** Option.

Verhalten überprüfen:

Wenn Host-A (192.168.1.40) versucht, eine HTTP-Sitzung mit Host-B (192.168.2.40) herzustellen, zeigt die LINA-Eingangserfassung Folgendes an:

```
firepower# show capture CAPI
```

8 packets captured

```
1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
2: 11:31:19.826403 192.168.2.40.80 > 192.168.1.40.32790: S 1283931030:1283931030(0) ack
357753152 win 2896 <mss 1380,sackOK,timestamp 5449236 5450579>
3: 11:31:19.826556 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>
4: 11:31:20.026899 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450781 5449236>
5: 11:31:20.428887 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5451183 5449236>
...
```

Ausgangserfassung:

```
firepower# show capture CAPO
```

5 packets captured

```
1: 11:31:19.825869 192.168.1.40.32790 > 192.168.2.40.80: S 1163713179:1163713179(0) win 2920
<mss 1380,sackOK,timestamp 5450579 0>
2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
3: 11:31:23.426049 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5452836 5450579>
4: 11:31:29.426430 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5458836 5450579>
5: 11:31:41.427208 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5470836 5450579>
```

Die Ablaufverfolgung zeigt, dass das erste Paket (TCP SYN) von Snort zulässig ist, da das Anwendungserkennungsurteil noch nicht erreicht wurde:

```
firepower# show capture CAPI packet-number 1 trace
```

```
1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
...
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435461
```

```
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
```

```
access-list CSM_FW_ACL_ remark rule-id 268435461: L7 RULE: Rule1
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

...

Phase: 10

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 23194, packet dispatched to next module

...

Phase: 12

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Trace:

Packet: TCP, SYN, seq 357753151

AppID: service unknown (0), application unknown (0)

Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0

Firewall: **pending rule-matching, id 268435461, pending AppID**

NAP id 1, IPS id 0, **Verdict PASS**

Snort Verdict: (pass-packet) allow this packet

Result:

input-interface: OUTSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

output-line-status: up

Action: allow

Dasselbe gilt für das TCP SYN/ACK-Paket:

```
firepower# show capture CAPO packet-number 2 trace
```

```
2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack 1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
```

...

Phase: 3

Type: FLOW-LOOKUP

Subtype:

Result: ALLOW

Config:

Additional Information:

Found flow with id 23194, using existing flow

...

Phase: 5

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Trace:

Packet: TCP, SYN, ACK, seq 1283931030, ack 357753152

AppID: service unknown (0), application unknown (0)

Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0

Firewall: **pending rule-matching, id 268435461, pending AppID**

NAP id 1, IPS id 0, **Verdict PASS**

Snort Verdict: (pass-packet) allow this packet

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

```
output-interface: INSIDE
output-status: up
output-line-status: up
Action: allow
```

Snort gibt ein DROP-Urteil zurück, sobald eine Überprüfung des dritten Pakets abgeschlossen ist:

```
firepower# show capture CAPI packet-number 3 trace
  3: 11:31:19.826556 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 23194, using existing flow

Phase: 5
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 357753152, ack 1283931031
AppID: service HTTP (676), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0, vlan 0, sgt 65535, user 9999997,
url http://192.168.2.40/128k.html
Firewall: block rule, id 268435461, drop
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall
Snort Verdict: (block-list) block list this flow

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

Sie können den Befehl auch ausführen `system support trace` aus dem FTD CLISH-Modus. Dieses Tool bietet 2 Funktionen:

- Zeigt das Snort-Verdict für jedes Paket, das an die Datenerfassungsbibliothek (Data Acquisition Library, DAQ) gesendet und in LINA angezeigt wird. DAQ ist eine Komponente, die sich zwischen der FTD LINA-Engine und der Snort-Engine befindet.
- Ermöglicht die Ausführung `system support firewall-engine-debug` um zu sehen, was innerhalb der Snort-Engine selbst passiert.

Hier ist die Ausgabe:

```
> system support trace
```

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
```

Please specify a server IP address: **192.168.2.40**

Please specify a server port:

Enable firewall-engine-debug too? [n]: **y**

Monitoring packet tracer debug messages

Tracing enabled by Lina

```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, seq 2620409313
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 New session
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS
```

Tracing enabled by Lina

```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, ACK, seq 3700371680, ack 2620409314
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS
```

Tracing enabled by Lina

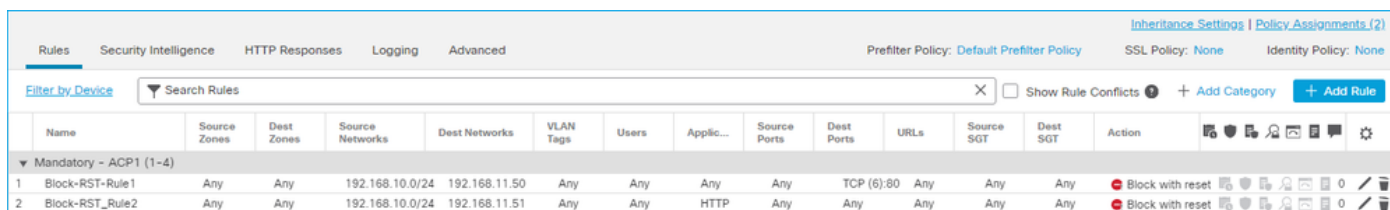
```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, ACK, seq 2620409314, ack 3700371681
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc
676, payload 0, client 686, misc 0, user 9999997, url http://192.168.2.40/128k.html, xff
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0)
-> 0, vlan 0, sgt 65535, user 9999997, url http://192.168.2.40/128k.html
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 match rule order 2, 'Rule1', action Block
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 deny action
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: block rule, 'Rule1', drop
192.168.1.40-32791 > 192.168.2.40-80 6 Snort: processed decoder alerts or actions queue, drop
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Deleting session
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict BLOCKLIST
192.168.1.40-32791 > 192.168.2.40-80 6 ==> Blocked by Firewall
```

Zusammenfassung

- Die ACP-Blockaktion wird in LINA entweder als Zulassen- oder als Ablehnungsregel bereitgestellt, was von den Regelbedingungen abhängt.
- Sind die Bedingungen L3/L4, blockiert LINA das Paket. Bei TCP wird das erste Paket (TCP SYN) blockiert.
- Wenn die Bedingungen L7 sind, wird das Paket zur weiteren Überprüfung an die Snort-Engine weitergeleitet. Im Fall von TCP werden einige Pakete über FTD zugelassen, bis Snort zu einem Urteil gelangt. Die zulässigen Pakete unterliegen weiterhin der Prüfung der Angriffsrichtlinie, die auf dem Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined' Option.

ACP-Block mit Rücksetzaktion

Ein Block mit auf der FMC-Benutzeroberfläche konfigurierter Ruheregel:



Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
Mandatory - ACP1 (1-4)													
1	Block-RST-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Block with reset
2	Block-RST_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Block with reset

Die Regel "Block mit Zurücksetzen" wird auf der FTD LINA-Engine als **permit** und die Snort-Engine als **reset** Regel:

```
firepower# show access-list
```

```
...
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=0) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Block-RST_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Snort-Engine:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
...
# Start of AC rule.
268438864 reset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 reset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

Wenn ein Paket mit einer Rücksetzregel übereinstimmt, sendet FTD eine **TCP Reset Paket** oder **ICMP Type 3 Code 13** Nachricht für nicht erreichbares Ziel (administrativ gefiltert):

```
root@kali:~/tests# wget 192.168.11.50/file1.zip
--2020-06-20 22:48:10-- http://192.168.11.50/file1.zip
Connecting to 192.168.11.50:80... failed: Connection refused.
```

Hier eine Aufnahme der FTD-Eingangsschnittstelle:

```
firepower# show capture CAPI
2 packets captured
1: 21:01:00.977259 802.1Q vlan#202 P0 192.168.10.50.41986 > 192.168.11.50.80: S
3120295488:3120295488(0) win 29200 <mss 1460,sackOK,timestamp 3740873275 0,nop,wscale 7>
2: 21:01:00.978114 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.41986: R 0:0(0) ack
3120295489 win 0 2 packets shown
```

System support trace zeigt in diesem Fall, dass das Paket aufgrund des Snort-Urteils verworfen wurde:

> **system support trace**

Enable firewall-engine-debug too? [n]: **y**

Please specify an IP protocol: **tcp**

Please specify a client IP address: **192.168.10.50**

Please specify a client port:

Please specify a server IP address: **192.168.11.50**

Please specify a server port:

Monitoring packet tracer and firewall debug messages

```
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3387496622
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 new firewall session
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 using HW or preset rule order 2, 'Block-RST-
Rule1', action Reset and prefilter rule 0
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 HitCount data sent for rule id: 268438864,
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 reset action
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 deleting firewall session flags = 0x0,
fwFlags = 0x0
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: block w/ reset rule, 'Block-RST-
Rule1', drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 9, NAP id 1, IPS id 0, Verdict
BLOCKLIST
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

Anwendungsbeispiele

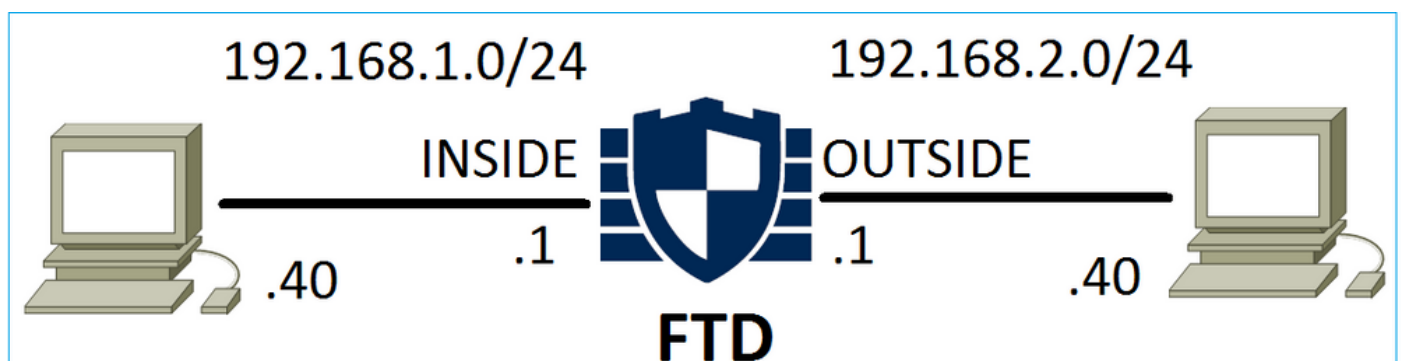
Identisch mit **Block** -Aktion, beendet aber sofort die Verbindung.

ACP-Zulassungsaktion

Szenario 1. ACP-Zulassungsaktion (L3/L4-Bedingungen)

Normalerweise konfigurieren Sie eine Zulassungsregel, um zusätzliche Inspektionen wie eine Angriffsrichtlinie und/oder eine Dateirichtlinie anzugeben. Dieses erste Szenario veranschaulicht den Betrieb einer Zulassungsregel, wenn eine L3/L4-Bedingung angewendet wird.

Betrachten Sie diese Topologie wie in der Abbildung dargestellt:



Diese Richtlinie wird wie im Bild gezeigt angewendet:

Access Control > Access Control													
Network Discovery			Application Detectors			Correlation			Actions				
ACP1													
Enter Description													
Prefilter Policy: Default Prefilter Policy				SSL Policy: None				Identity Policy: None					
Inheritance Settings													
Rules Security Intelligence HTTP Responses Advanced													
Filter by Device <input type="checkbox"/> Show Rule Conflicts <input type="checkbox"/> Add Category <input type="button" value="+"/> Add Rule <input type="button" value="Search Rules"/>													
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	Allow

Die bereitgestellte Richtlinie in Snort. Beachten Sie, dass die Regel als **allow** aktion:

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

Die Politik in LINA.

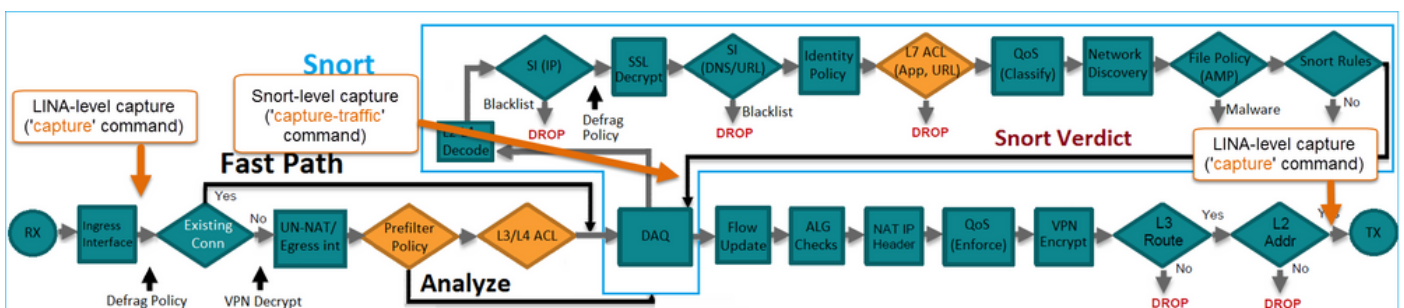
Anmerkung: Die Regel wird als **permit** Aktion, die im Wesentlichen eine Weiterleitung an Snort zur weiteren Überprüfung bedeutet.

```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 (hitcnt=1) 0x641a20c3
```

Um zu sehen, wie FTD einen Fluss behandelt, der mit einer Zulassungsregel übereinstimmt, gibt es mehrere Möglichkeiten:

- Snort-Statistik überprüfen
- Mit dem System-Support trace CLISH Tool
- Mit der Capture-Option in LINA und optional mit Capture-Traffic in der Snort Engine

LINA-Erfassung und Snort-Erfassungsverkehr:



Verhalten überprüfen:

Snort-Statistik löschen, aktivieren **system support trace** from CLISH, and initiate an HTTP flow from host-A (192.168.1.40) to host-B (192.168.2.40). All the packets are forwarded to the Snort engine and get the PASS verdict by the Snort:

```
firepower# clear snort statistics
```

```
> system support trace
```

```
Please specify an IP protocol:
```

```
Please specify a client IP address: 192.168.1.40
```

```
Please specify a client port:
```

```
Please specify a server IP address: 192.168.2.40
```

```
Please specify a server port:
```

```
Enable firewall-engine-debug too? [n]:
```

```
Monitoring packet tracer debug messages
```

```
Tracing enabled by Lina
```

```
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, seq 361134402
```

```
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
```

```
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
```

```
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
```

```
Trace buffer and verdict reason are sent to DAQ's PDTS
```

```
Tracing enabled by Lina
```

```
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, ACK, seq 1591434735, ack 361134403
```

```
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
```

```
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
```

```
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
```

```
Trace buffer and verdict reason are sent to DAQ's PDTS
```

```
Tracing enabled by Lina
```

```
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, ACK, seq 361134403, ack 1591434736
```

```
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service HTTP (676), application unknown (0)
```

```
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
```

```
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
```

Die Zähler für "Pakete passieren" werden erhöht:

```
> show snort statistics
```

```
Packet Counters:
```

Passed Packets	54
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

```
Flow Counters:
```

Fast-Forwarded Flows	0
Blocklisted Flows	0

```
...
```

Erfolgreiche Pakete = Vom Snort-Modul überprüft

Szenario 2. ACP-Zulassungsaktion (L3-7-Bedingungen)

Ein ähnliches Verhalten tritt auf, wenn die Zulassungsregel wie folgt bereitgestellt wird.

Nur eine L3/L4-Bedingung, wie im Bild dargestellt:

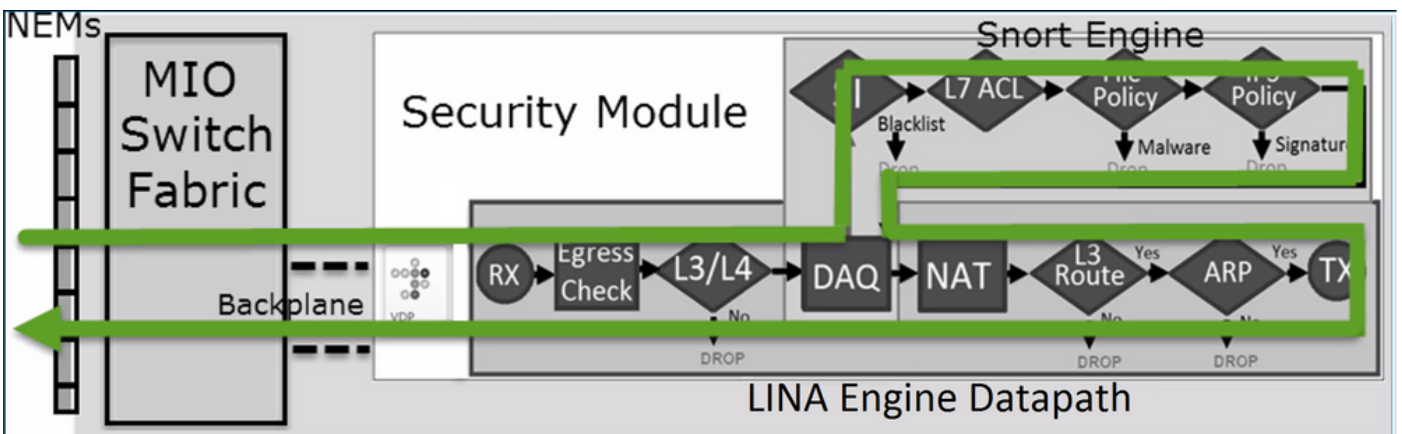
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
▼ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

Eine L7-Bedingung (z. B. Richtlinie für Sicherheitsrisiken, Dateirichtlinie, Anwendung usw.) wird im Bild angezeigt:

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
▼ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

Zusammenfassung

Zusammenfassend lässt sich feststellen, dass ein auf einem FP4100/9300 bereitgestellter FTD-Datenstrom so behandelt wird, wenn eine Zulassungsregel zugeordnet wird, wie im Bild gezeigt:



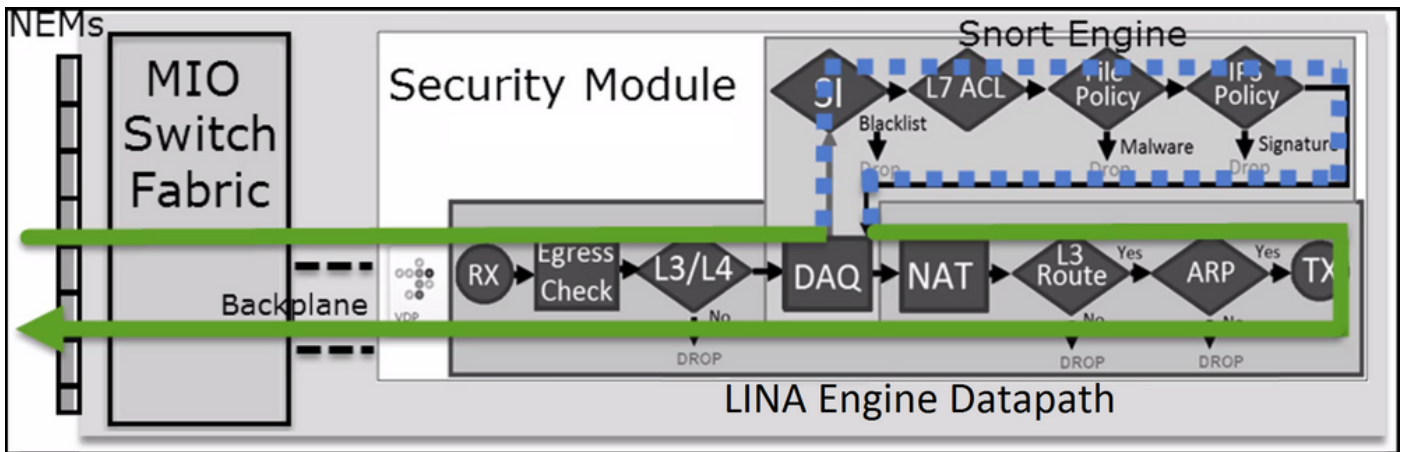
Anmerkung: Management Input Output (MIO) ist die Supervisor Engine des Firepower-Chassis.

Szenario 3. Snort Fast-Forward-Verdict mit Allow

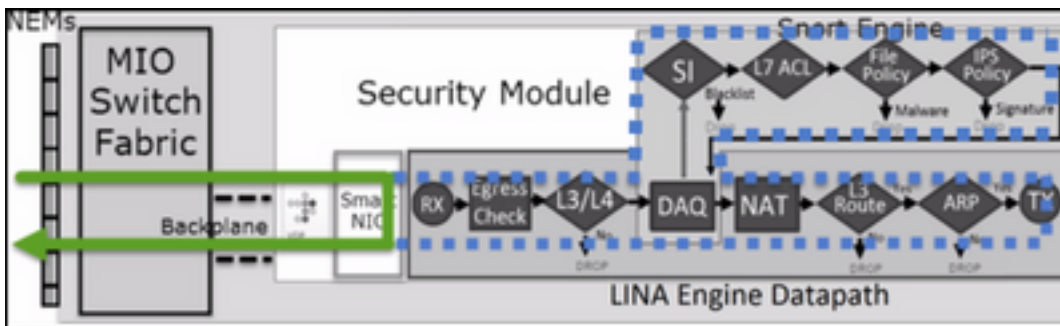
Es gibt bestimmte Szenarien, in denen die FTD Snort Engine ein PERMITLIST-Urteil abgibt (Fast-Forward) und der restliche Fluss an die LINA Engine ausgelagert wird (in einigen Fällen dann an den HW Accelerator - SmartNIC ausgelagert wird). Diese sind:

1. SSL-Datenverkehr ohne konfigurierte SSL-Richtlinie
2. Intelligent Application Bypass (IAB)

Dies ist die visuelle Darstellung des Paketpfads:



Oder in einigen Fällen:



Wichtigste Punkte

- Die Zulassungsregel wird bereitgestellt als **allow** in Snort und **permit** in LINA
- In den meisten Fällen werden alle Pakete einer Sitzung zur zusätzlichen Überprüfung an die Snort-Engine weitergeleitet.

Anwendungsbeispiele

Sie konfigurieren eine Zulassungsregel, wenn Sie eine L7-Überprüfung durch die Snort Engine benötigen. Beispiel:

- Richtlinie für Sicherheitsrisiken
- Dateirichtlinie

AKP-Treuhandaktion

Szenario 1. ACP Trust Action

Wenn Sie keine erweiterte L7-Inspektion auf Snort-Ebene anwenden möchten (z. B. Intrusion Policy, File Policy, Network Discovery), aber dennoch Funktionen wie Security Intelligence (SI), Identity Policy, QoS usw. verwenden möchten, wird empfohlen, die Trust-Aktion in Ihrer Regel zu verwenden.

Topologie:



Die konfigurierte Richtlinie:

ACP1															Analyze Hit Counts	Save	Cancel	
Enter Description															Inheritance Settings Policy Assignments (1)			
Rules	Security Intelligence	HTTP Responses	Logging	Advanced	Prefilter Policy: Prefilter1					SSL Policy: None		Identity Policy: None						
Filter by Device															Search Rules	Show Rule Conflicts	Add Category	Add Rule
Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action					
Mandatory - ACP1 (1-4)																		
1	trust_L3-L4	Any	Any	192.168.10.50 192.168.10.51	192.168.11.50 192.168.11.51	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Trust				

Die Trust-Regel in der FTD Snort Engine:

```
# Start of AC rule.
268438858 fastpath any 192.168.10.50 31 any any 192.168.11.50 31 80 any 6 (log dcforward
flowend)
```

Anmerkung: Die Zahl 6 ist das Protokoll (TCP).

Die Regel in FTD LINA:

```
firepower# show access-list | i 268438858
access-list CSM_FW_ACL_ line 17 remark rule-id 268438858: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 18 remark rule-id 268438858: L7 RULE: trust_L3-L4
access-list CSM_FW_ACL_ line 19 advanced permit tcp object-group FMC_INLINE_src_rule_268438858
object-group FMC_INLINE_dst_rule_268438858 eq www rule-id 268438858 (hitcnt=19) 0x29588b4f
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=19) 0x9d442895
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0xd026252b
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=0) 0x0d785cc4
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0x3b3234f1
```

Bestätigung:

Aktivieren `system support trace` und eine HTTP-Sitzung von Host-A (192.168.10.50) zu Host-B (192.168.11.50) initiieren. Es werden 3 Pakete an die Snort-Engine weitergeleitet. Snort Engine sendet an LINA das PERMITLIST-Urteil, das im Wesentlichen den Rest des Flusses an die LINA-

Engine auslagert:

> **system support trace**

Enable firewall-engine-debug too? [n]: **y**

Please specify an IP protocol: **tcp**

Please specify a client IP address: **192.168.10.50**

Please specify a client port:

Please specify a server IP address: **192.168.11.50**

Please specify a server port: **80**

Monitoring packet tracer and firewall debug messages

```
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 453426648
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 new firewall session
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 using HW or preset rule order 5, 'trust_L3-
L4', action Trust and prefilter rule 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 HitCount data sent for rule id: 268438858,
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2820426532, ack
453426649
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 453426649, ack
2820426533
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PERMITLIST
```

Sobald die Verbindung beendet ist, ruft das Snort-Modul die Metadateninformationen vom LINA-Modul ab und löscht die Sitzung:

```
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 3
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Logging EOF for event from hardware with
rule_id = 268438858 ruleAction = 3 ruleReason = 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 : Received EOF, deleting the snort session.

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleting snort session, reason:
timeout
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 deleting firewall session flags = 0x10003,
fwFlags = 0x1115
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleted snort session using 0
bytes; protocol id:(-1) : LWstate 0xf LWFlags 0x6007
```

Snort Capture zeigt die 3 Pakete, die an die Snort Engine gehen:

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - management0
- 1 - management1
- 2 - Global

```
Selection? 2
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options: -n vlan and (host 192.168.10.50 and host 192.168.11.50)
```

```
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [S], seq 3065553465, win 29200, options [mss 1380,sackOK,TS val 3789188468 ecr 0,nop,wscale 7], length 0
```

```
10:26:16.525928 IP 192.168.11.50.80 > 192.168.10.50.42144: Flags [S.], seq 3581351172, ack 3065553466, win 8192, options [mss 1380,nop,wscale 8,sackOK,TS val 57650410 ecr 3789188468], length 0
```

```
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [.], ack 1, win 229, options [nop,nop,TS val 3789188470 ecr 57650410], length 0
```

Die LINA-Aufzeichnung zeigt den durchlaufenden Fluss:

```
firepower# show capture CAPI
```

```
437 packets captured
```

```
1: 09:51:19.431007 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: S
2459891187:2459891187(0) win 29200 <mss 1460,sackOK,timestamp 3787091387 0,nop,wscale 7>
2: 09:51:19.431648 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: S
2860907367:2860907367(0) ack 2459891188 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
57440579 3787091387>
3: 09:51:19.431847 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: . ack
2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
4: 09:51:19.431953 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: P
2459891188:2459891337(149) ack 2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
5: 09:51:19.444816 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860907368:2860908736(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>
6: 09:51:19.444831 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860908736:2860910104(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>
```

```
...
```

Die Nachverfolgung der Pakete von LINA ist eine weitere Möglichkeit, die Snort-Urteile zu sehen. Das erste Paket erhielt das PASS-Urteil:

```
firepower# show capture CAPI packet-number 1 trace | i Type|Verdict
```

```
Type: CAPTURE
Type: ACCESS-LIST
Type: ROUTE-LOOKUP
Type: ACCESS-LIST
Type: CONN-SETTINGS
Type: NAT
Type: NAT
Type: IP-OPTIONS
Type: CAPTURE
Type: CAPTURE
Type: NAT
Type: CAPTURE
```

Type: NAT
Type: IP-OPTIONS
Type: CAPTURE
Type: FLOW-CREATION
Type: EXTERNAL-INSPECT

Type: SNORT

Snort id 22, NAP id 2, IPS id 0, Verdict PASS

Snort Verdict: (pass-packet) allow this packet

Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP

Type: ADJACENCY-LOOKUP

Type: CAPTURE

Nachverfolgung des TCP-SYN/ACK-Pakets an der OUTSIDE-Schnittstelle:

```
firepower# show capture CAPO packet-number 2 trace | i Type|Verdict
```

Type: CAPTURE

Type: ACCESS-LIST

Type: FLOW-LOOKUP

Type: EXTERNAL-INSPECT

Type: SNORT

Snort id 22, NAP id 2, IPS id 0, Verdict PASS

Snort Verdict: (pass-packet) allow this packet

Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP

Type: ADJACENCY-LOOKUP

Type: CAPTURE

Die TCP ACK erhält das PERMITLIST-Urteil:

```
firepower# show capture CAPI packet-number 3 trace | i Type|Verdict
```

Type: CAPTURE

Type: ACCESS-LIST

Type: FLOW-LOOKUP

Type: EXTERNAL-INSPECT

Type: SNORT

Snort id 22, NAP id 2, IPS id 0, Verdict PERMITLIST

Snort Verdict: (fast-forward) fast forward this flow

Type: CAPTURE

Dies ist die vollständige Ausgabe des Snort Verdict (Paket #3)

```
firepower# show capture CAPI packet-number 3 trace | b Type: SNORT
```

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Trace:

Packet: TCP, ACK, seq 687485179, ack 1029625865

AppID: service unknown (0), application unknown (0)

Firewall: trust/fastpath rule, id 268438858, allow

Snort id 31, NAP id 2, IPS id 0, **Verdict PERMITLIST**

Snort Verdict: (fast-forward) fast forward this flow

Das vierte Paket wird nicht an die Snort-Engine weitergeleitet, da das Urteil von der LINA-Engine zwischengespeichert wird:

firepower# **show capture CAPI packet-number 4 trace**

441 packets captured

4: 10:34:02.741523 802.1Q vlan#202 PO 192.168.10.50.42158 > 192.168.11.50.80: P
164375589:164375738(149) ack 3008397532 win 229 <nop,nop,timestamp 3789654678 57697031>

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: FLOW-LOOKUP

Subtype:

Result: ALLOW

Config:

Additional Information:

Found flow with id 1254, using existing flow

Phase: 4

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Verdict: (fast-forward) fast forward this flow

Result:

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

Action: allow

1 packet shown

Snort-Statistiken bestätigen dies:

firepower# **show snort statistics**

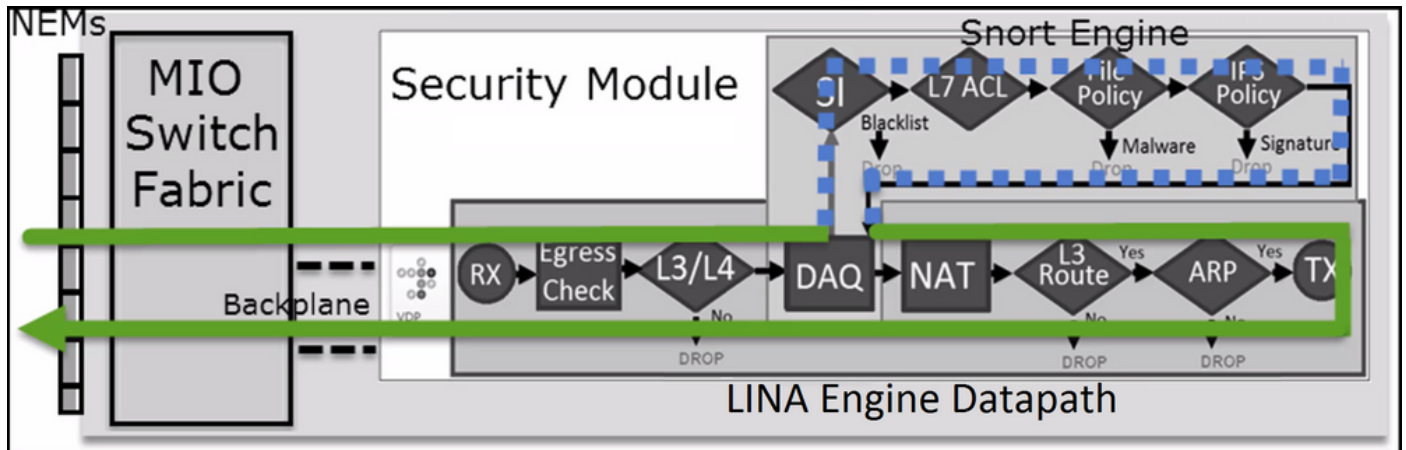
Packet Counters:

Passed Packets	2
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

Flow Counters:

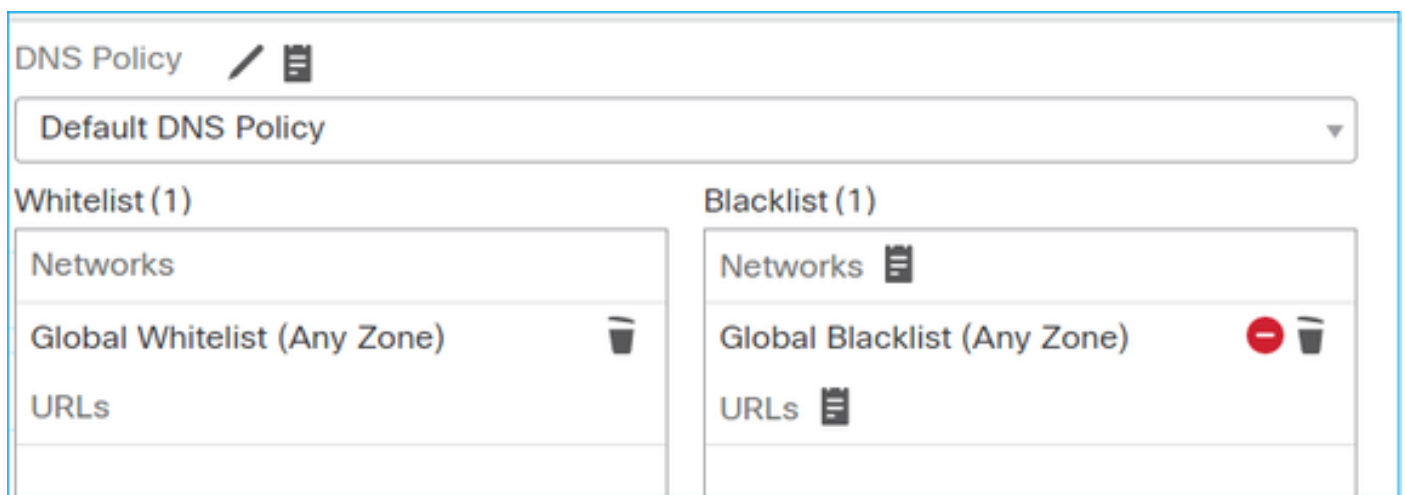
Fast-Forwarded Flows	1
Blacklisted Flows	0
Miscellaneous Counters:	
Start-of-Flow events	0
End-of-Flow events	1
Denied flow events	0
Frames forwarded to Snort before drop	0
Inject packets dropped	0

Paketfluss mit Vertrauensregel. Einige Pakete werden von Snort geprüft, die übrigen von LINA:



Szenario 2. ACP Trust Action (ohne SI, QoS und Identitätsrichtlinie)

Wenn Sie möchten, dass die FTD Sicherheitsinsprüfungen (SI) auf alle Datenflüsse anwendet, ist SI bereits auf ACP-Ebene aktiviert und Sie können die SI-Quellen (TALOS, Feeds, Listen usw.) angeben. Wenn Sie sie jedoch deaktivieren möchten, deaktivieren Sie SI für Netzwerke global per ACP, SI für URL und SI für DNS. Die SI für Netzwerke und die URL ist deaktiviert, wie in der Abbildung dargestellt:



In diesem Fall wird die Trust-Regel in LINA als trust bereitgestellt:

```
> show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
```

Anmerkung: Ab 6.2.2 unterstützt FTD TID. TID funktioniert ähnlich wie SI, aber falls SI deaktiviert ist, erzwingt es keine Paketumleitung zur Snort-Engine zur TID-Prüfung.

Überprüfung des Verhaltens

Starten Sie eine HTTP-Sitzung von Host-A (192.168.1.40) zu Host-B (192.168.2.40). Da es sich um einen FP4100 handelt, der Flow Offload in der Hardware unterstützt, geschieht Folgendes:

- Einige Pakete werden über die FTD LINA-Engine weitergeleitet, und der Rest des Datenflusses wird an SmartNIC (HW Accelerator) ausgelagert.
- Keine Pakete an die Snort-Engine weitergeleitet

Die FTD LINA-Verbindungstabelle zeigt das Flago' was bedeutet, dass der Fluss an HW ausgelagert wurde. Beachten Sie auch, dass dasn". Dies bedeutet im Wesentlichen "keine Snort-Umleitung":

```
firepower# show conn
1 in use, 15 most used
```

```
TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:32809, idle 0:00:00, bytes 949584, flags UIOo
```

Snort-Statistiken zeigen nur protokollierte Ereignisse zu Beginn und am Ende der Sitzung:

```
firepower# show snort statistics
```

Packet Counters:

Passed Packets	0
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

Flow Counters:

Fast-Forwarded Flows	0
Blacklisted Flows	0

Miscellaneous Counters:

Start-of-Flow events	1
End-of-Flow events	1

FTD LINA-Protokolle zeigen, dass für jede Sitzung zwei Datenflüsse (einer pro Richtung) an die HW ausgelagert wurden:

```
Sep 27 2017 20:16:05: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Sep 27 2017 20:16:05: %ASA-6-302013: Built inbound TCP connection 25384 for
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
```

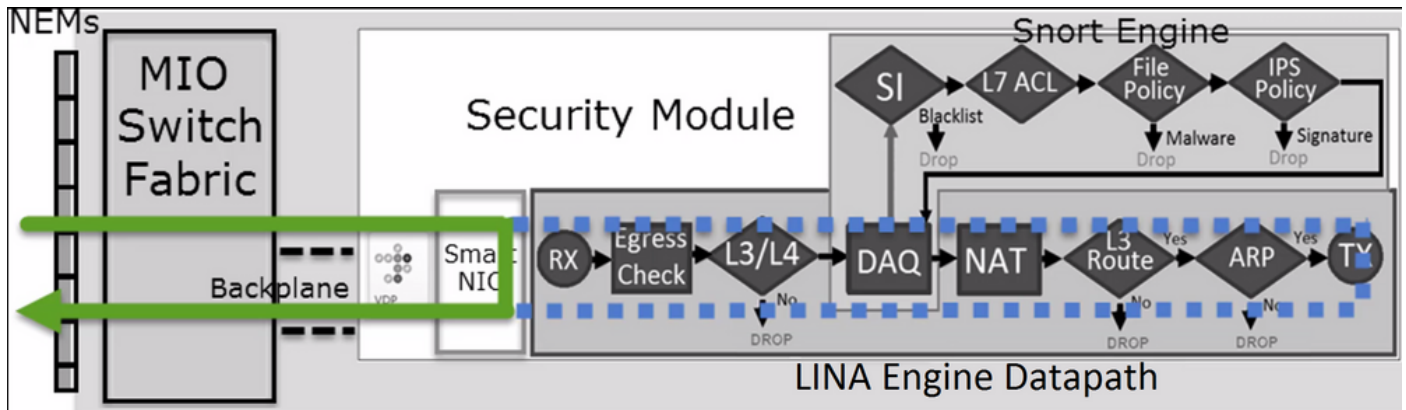


```

INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-302014: Teardown TCP connection 25384 for INSIDE:192.168.1.40/32809
to OUTSIDE:192.168.2.40/80 duration 0:00:00 bytes 1055048 TCP FINs
Sep 27 2017 20:16:05: %ASA-7-609002: Teardown local-host INSIDE:192.168.1.40 duration 0:00:00

```

Paketfluss mit Trust Rule bereitgestellt als **trust** Aktion in LINA. Einige Pakete werden von LINA geprüft, der Rest wird an SmartNIC ausgelagert (FP4100/FP9300):

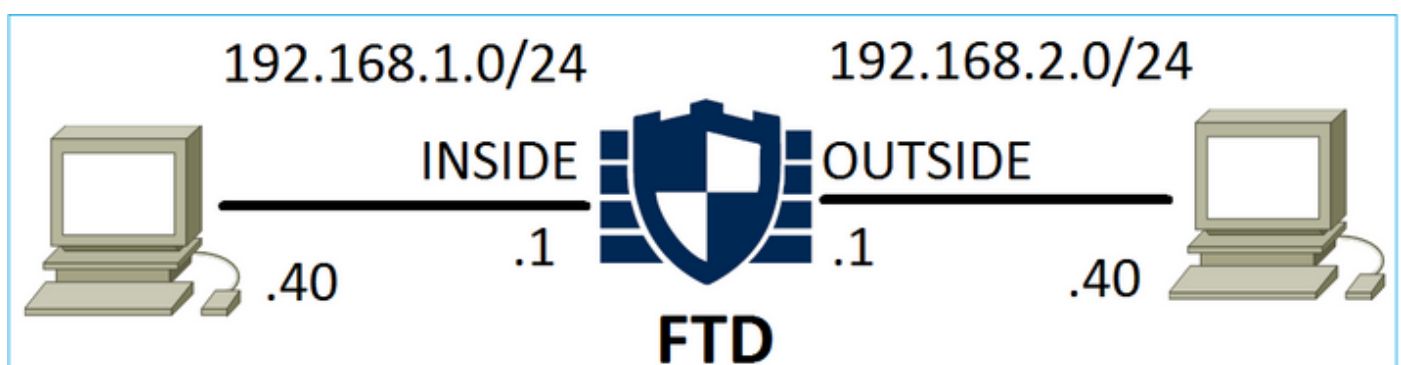


Anwendungsbeispiele

- Sie müssen **Trust** -Aktion, wenn nur wenige Pakete von der Snort-Engine geprüft werden sollen (z. B. Anwendungserkennung, SI-Prüfung) und der restliche Fluss an die LINA-Engine ausgelagert werden soll.
- Wenn Sie FTD auf FP4100/9300 verwenden und möchten, dass der Fluss die Snort-Inspektion vollständig umgeht, sollten Sie die Prefilter-Regel mit **Fastpath** Aktion (siehe den zugehörigen Abschnitt in diesem Dokument)

Sperren von Richtlinien vorfiltern

Betrachten Sie die Topologie wie im Bild gezeigt:



Beachten Sie auch die Richtlinie, wie im Bild gezeigt:

Access Control ▶ Prefilter		Network Discovery	Application Detectors	Correlation	Actions ▼				
FTD_Prefilter									
Enter Description									
Rules									
				+ Add Tunnel Rule	+ Add Prefilter Rule				
Search Rules									
#	Name	Rule T...	...	De Source In Networks	Destination Networks	Source Port	Destinat... Port	VLAN Tag	Action
1	Prefilter1	Prefilter	any any	192.168.1.40	192.168.2.40	any	any	any	Block

Dies ist die bereitgestellte Richtlinie im FTD Snort-Modul (Datei "ngfw.rules"):

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268437506 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any (tunnel -1
```

In LINA:

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id
268437506 event-log flow-start (hitcnt=0) 0x76476240
```

Wenn Sie ein virtuelles Paket verfolgen, zeigt dies, dass das Paket von LINA verworfen und nie an Snort weitergeleitet wird:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id 268437506
event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ remark rule-id 268437506: RULE: Prefilter1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Snort-Statistiken zeigen:

```
firepower# show snort statistics
```

```

Packet Counters:
  Passed Packets                                0
  Blocked Packets                               0
  Injected Packets                             0
  Packets bypassed (Snort Down)                0
  Packets bypassed (Snort Busy)                0

Flow Counters:
  Fast-Forwarded Flows                         0
  Blacklisted Flows                            0

Miscellaneous Counters:
  Start-of-Flow events                         0
  End-of-Flow events                           0
  Denied flow events                          1

```

LINA ASP-Drops zeigen:

```
firepower# show asp drop
```

```

Frame drop:
  Flow is denied by configured rule (acl-drop)          1

```

Anwendungsbeispiele

Sie können eine Prefilter Block-Regel verwenden, wenn Sie Datenverkehr auf der Basis von L3/L4-Bedingungen blockieren möchten, ohne dass eine Snort-Überprüfung des Datenverkehrs durchgeführt werden muss.

Vorfilter-Policy Fastpath-Aktion

Berücksichtigen Sie die Vorfilterrichtlinie wie in der Abbildung dargestellt:

#	Name	Rule T...	Sou Int	De Int	Source Networks	Destination Networks	Source Port	Destinati...	VLAN Tag	Action
1	Prefilter1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	TCP (6):80	any	→ Fastpath

Dies ist die bereitgestellte Richtlinie in der FTD Snort Engine:

```
268437506 fastpath any any any any any any any (log dcforward flowend) (tunnel -1)
```

In FTD LINA:

```

access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced trust tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268437506 event-log flow-end (hitcnt=0) 0xf3410b6f

```

Verhalten überprüfen

Wenn Host-A (192.168.1.40) versucht, eine HTTP-Sitzung mit Host-B (192.168.2.40) zu öffnen, durchlaufen einige Pakete LINA, und der Rest wird an SmartNIC ausgelagert. In diesem Fall `system support trace` mit `firewall-engine-debug` Aktiviert zeigt:

```
> system support trace
```

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages
```

```
192.168.1.40-32840 > 192.168.2.40-80 6 AS 1 I 8 Got end of flow event from hardware with flags
04000000
```

LINA-Protokolle zeigen den Offload-Fluss an:

```
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host OUTSIDE:192.168.2.40
Oct 01 2017 14:36:51: %ASA-6-302013: Built inbound TCP connection 966 for
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32840 (192.168.1.40/32840)
```

LINA-Erfassungen zeigen, dass 8 Pakete Folgendes durchlaufen:

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
```

```
firepower# show capture CAPI
```

```
8 packets captured
```

```
  1: 14:45:32.700021 192.168.1.40.32842 > 192.168.2.40.80: S 3195173118:3195173118(0) win 2920
<mss 1460,sackOK,timestamp 332569060 0>
  2: 14:45:32.700372 192.168.2.40.80 > 192.168.1.40.32842: S 184794124:184794124(0) ack
3195173119 win 2896 <mss 1380,sackOK,timestamp 332567732 332569060>
  3: 14:45:32.700540 192.168.1.40.32842 > 192.168.2.40.80: P 3195173119:3195173317(198) ack
184794125 win 2920 <nop,nop,timestamp 332569060 332567732>
  4: 14:45:32.700876 192.168.2.40.80 > 192.168.1.40.32842: . 184794125:184795493(1368) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
```

```

5: 14:45:32.700922 192.168.2.40.80 > 192.168.1.40.32842: P 184795493:184796861(1368) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
6: 14:45:32.701425 192.168.2.40.80 > 192.168.1.40.32842: FP 184810541:184810851(310) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569061>
7: 14:45:32.701532 192.168.1.40.32842 > 192.168.2.40.80: F 3195173317:3195173317(0) ack
184810852 win 2736 <nop,nop,timestamp 332569061 332567733>
8: 14:45:32.701639 192.168.2.40.80 > 192.168.1.40.32842: . ack 3195173318 win 2697
<nop,nop,timestamp 332567734 332569061>

```

FTD-Flow-Offload-Statistiken zeigen 22 an HW ausgelagerte Pakete:

```

firepower# show flow-offload statistics
Packet stats of port : 0
Tx Packet count      :                22
Rx Packet count      :                22
Dropped Packet count :                0
VNIC transmitted packet :                22
VNIC transmitted bytes :              15308
VNIC Dropped packets  :                0
VNIC erroneous received :                0
VNIC CRC errors       :                0
VNIC transmit failed  :                0
VNIC multicast received :                0

```

Sie können auch die `show flow-offload flow` um zusätzliche Informationen zu den ausgelagerten Flows anzuzeigen. Hier ein Beispiel:

```

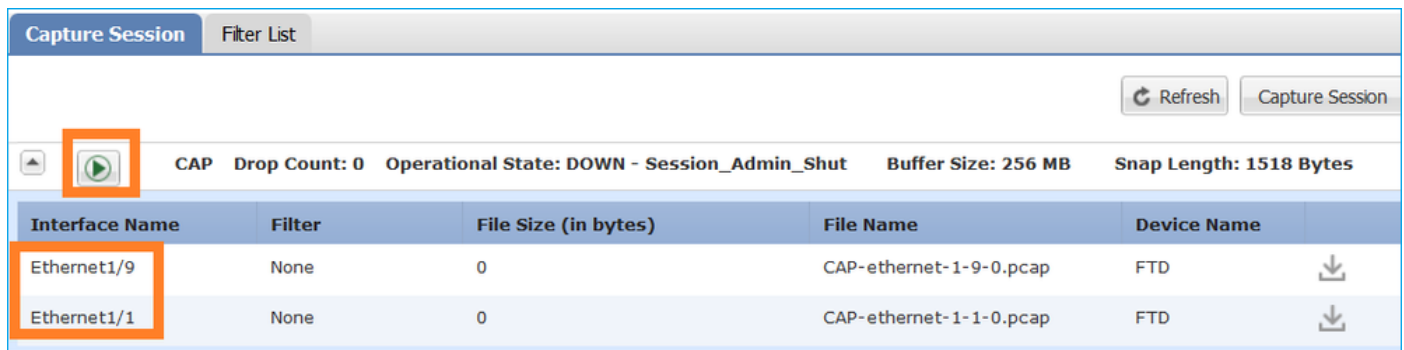
firepower# show flow-offload flow
Total offloaded flow stats: 2 in use, 4 most used, 20% offloaded, 0 collisions
TCP intf0 103 src 192.168.1.40:39301 dest 192.168.2.40:20, static, timestamp 616063741, packets
33240, bytes 2326800
TCP intf0 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 616063760, packets
249140, bytes 358263320
firepower# show conn
5 in use, 5 most used
Inspect Snort:
  preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 0 most in effect

TCP OUTSIDE 192.168.2.40:21 INSIDE 192.168.1.40:40988, idle 0:00:00, bytes 723, flags UIO
TCP OUTSIDE 192.168.2.40:21 INSIDE 192.168.1.40:40980, idle 0:02:40, bytes 1086, flags UIO
TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:49442, idle 0:00:00, bytes 86348310, flags UIO
N1
TCP OUTSIDE 192.168.2.40:20 INSIDE 192.168.1.40:39301, idle 0:00:00, bytes 485268628, flags Uo
<- offloaded flow
TCP OUTSIDE 192.168.2.40:20 INSIDE 192.168.1.40:34713, idle 0:02:40, bytes 821799360, flags
UFRIO

```

- Der Prozentsatz basiert auf dem 'show conn' output. Wenn beispielsweise insgesamt 5 Verbindungen die FTD LINA-Engine durchlaufen und 1 davon ausgelagert wird, werden 20 % als ausgelagert gemeldet.
- Die Höchstgrenze für ausgelagerte Sitzungen hängt von der Softwareversion ab (z. B. unterstützen ASA 9.8.3 und FTD 6.2.3 4 Millionen bidirektionale (oder 8 Millionen unidirektionale) ausgelagerte Datenströme).
- Erreicht die Anzahl der ausgelagerten Datenflüsse den Grenzwert (z. B. 4 Millionen bidirektionale Datenflüsse), werden keine neuen Verbindungen ausgelagert, bis die aktuellen Verbindungen aus der ausgelagerten Tabelle entfernt werden.

Um alle Pakete auf FP4100/9300 zu sehen, die FTD durchlaufen (ausgelagert + LINA), muss die Erfassung auf Chassis-Ebene aktiviert werden, wie im Bild gezeigt:



Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/9	None	0	CAP-ethernet-1-9-0.pcap	FTD
Ethernet1/1	None	0	CAP-ethernet-1-1-0.pcap	FTD

Die Erfassung der Chassis-Rückwandplatine zeigt beide Richtungen. Aufgrund der FXOS-Erfassungsarchitektur (2 Erfassungspunkte pro Richtung) wird jedes Paket **zweimal** angezeigt, wie im Bild gezeigt:

Paketstatistiken:

- Gesamtpakete über FTD: 30
- Pakete über FTD LINA: 8
- Pakete werden an SmartNIC HW Accelerator ausgelagert: 22

Bei einer anderen Plattform als FP4100/FP9300 werden alle Pakete von der LINA-Engine verarbeitet, da Flow-Offload nicht unterstützt wird (beachten Sie das Fehlen des **o**-Flags):

```
FP2100-6# show conn addr 192.168.1.40
33 in use, 123 most used
Inspect Snort:
    preserve-connection: 0 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:50890, idle 0:00:09, bytes 175, flags UxIO
```

Die LINA-Syslogs zeigen nur Ereignisse beim Verbindungsaufbau und Verbindungsabschluss an:

```
FP2100-6# show log | i 192.168.2.40
Jun 21 2020 14:29:44: %FTD-6-302013: Built inbound TCP connection 6914 for
INSIDE:192.168.1.40/50900 (192.168.11.101/50900) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Jun 21 2020 14:30:30: %FTD-6-302014: Teardown TCP connection 6914 for INSIDE:192.168.1.40/50900
to OUTSIDE:192.168.2.40/80 duration 0:00:46 bytes 565 TCP FINs from OUTSIDE
```

Anwendungsbeispiele

- Nutzung **Prefilter Fastpath** -Aktion, wenn Sie die Snort-Inspektion vollständig umgehen möchten. Dies ist in der Regel bei großen vertrauenswürdigen Datenflüssen (z. B. Backups, Datenbankübertragungen usw.) ratsam.
- Auf FP4100/9300-Appliances **Fastpath** löst Flow-Offload aus, und nur wenige Pakete durchlaufen die FTD LINA-Engine. Der Rest wird von SmartNIC übernommen, wodurch die Latenz verringert wird.

Fastpath-Aktion der Vorfiltrerrichtlinie (Inline-Set)

Falls eine Fastpath-Aktion der Vorfilterrichtlinie auf Datenverkehr angewendet wird, der einen Inline-Satz durchläuft (NGIPS-Schnittstellen), müssen diese Punkte berücksichtigt werden:

- Die Regel wird auf das LINA-Modul als `trust` Aktion
- Der Fluss wird nicht von der Snort-Engine überprüft.
- Flow Offload (HW-Beschleunigung) tritt nicht auf, da Flow Offload auf NGIPS-Schnittstellen nicht anwendbar ist.

Das folgende Beispiel zeigt eine Paketverfolgung im Fall einer Fastpath-Vorfilteraktion, die auf eine Inline-Gruppe angewendet wird:

```
firepower# packet-tracer input inside tcp 192.168.1.40 12345 192.168.1.50 80 detailed

Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
Forward Flow based lookup yields rule:
in id=0x2ad7ac48b330, priority=501, domain=ips-mode, deny=false
hits=2, user_data=0x2ad80d54abd0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip object 192.168.1.0 object 192.168.1.0 rule-id
268438531 event-log flow-end
access-list CSM_FW_ACL_ remark rule-id 268438531: PREFILTER POLICY: PF1
access-list CSM_FW_ACL_ remark rule-id 268438531: RULE: 1
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ad9f9f8a7f0, priority=12, domain=permit, trust
hits=1, user_data=0x2ad9b23c5d40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any
dst ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface inside is in NGIPS inline mode.
Egress interface outside is determined by inline-set configuration

Phase: 4
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7, packet dispatched to next module
```

```

Module information for forward flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

```

```

Module information for reverse flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

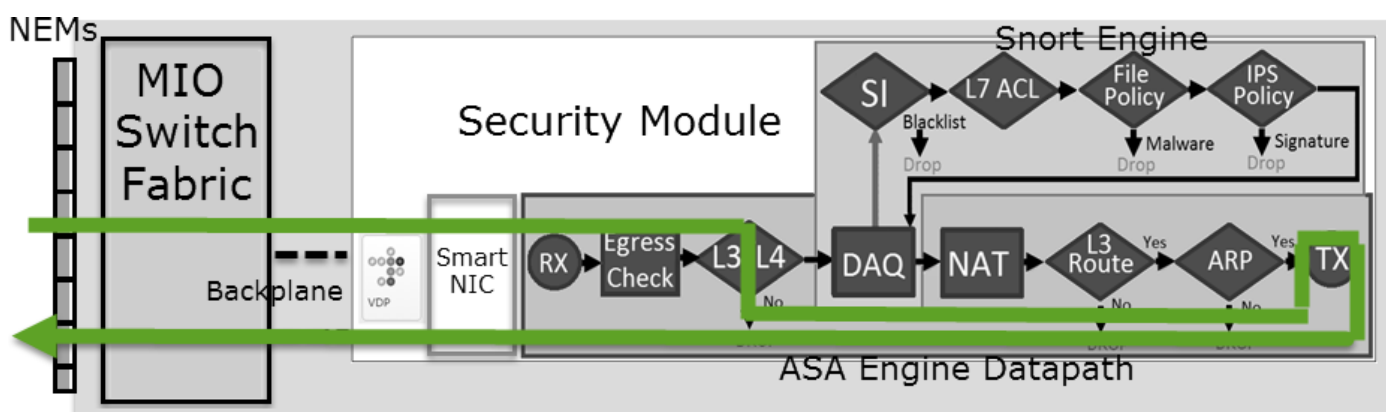
```

```

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow

```

Dies ist die visuelle Darstellung des Paketpfads:



Prefilter Policy FastPath Action (Inline-Set mit Tap)

Wie Inline-Set

Aktion zur Richtlinienanalyse vorfiltern

Szenario 1. Vorfilter Analyse mit ACP-Blockregel

Berücksichtigen Sie die Vorfilterrichtlinie, die eine Analyseregel enthält, wie im Bild gezeigt:

Access Control > Prefilter										
Prefilter_Policy1										
Enter Description										
Rules										
+ Add Tunnel Rule + Add Prefilter Rule Search R										
#	Name	Rule T...	Source Interfac...	Destinat... Interfac...	Source Networks	Destination Networks	Source Port	Destinat... Port	VLAN Tag	Action
1	Prefilter_Rule1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	any	any	Analyze

Der ACP enthält nur die Standardregel, die auf Block All Traffic wie im Bild gezeigt:

Access Control ▶ Access Control Network Discovery Application Detectors Correlation Actions ▼

ACP1
Enter Description

Prefilter Policy: Prefilter_Policy1 SSL Policy: None

Rules Security Intelligence HTTP Responses Advanced

Show Rule Conflicts

#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Action
▼ Mandatory - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
▼ Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action												Access Control: Block All Traffic	

Dies ist die bereitgestellte Richtlinie im FTD Snort-Modul (Datei "ngfw.rules"):

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268435460 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any (tunnel -1)
268435459 allow any any 1025-65535 any any 3544 any 17 (tunnel -1)
268435459 allow any any 3544 any any 1025-65535 any 17 (tunnel -1)
268435459 allow any any any any any any any 47 (tunnel -1)
268435459 allow any any any any any any any 41 (tunnel -1)
268435459 allow any any any any any any any 4 (tunnel -1)
# End of tunnel and priority rules.
# Start of AC rule.
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

Dies ist die in der FTD LINA-Engine bereitgestellte Richtlinie:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=0) 0xb788b786
```

Verhalten überprüfen

Packet-Tracer zeigt an, dass das Paket von LINA zugelassen und an die Snort-Engine weitergeleitet wird (aufgrund von **permit**) und Snort Engine gibt einen **Block** verdict, da die Standardaktion von AC abgeglichen wurde.

Anmerkung: Snort evaluiert den Datenverkehr nicht anhand von Tunnelregeln.

Wenn Sie ein Paket verfolgen, wird dasselbe angezeigt:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
```

```

access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

```

```

...
Phase: 14
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: block rule, id 268435458, drop
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall
Snort Verdict: (block-list) block list this flow

```

```

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor

```

Szenario 2. Vorfilter Analyse mit ACP-Zulassungsregel

Wenn das Ziel darin besteht, die Übertragung des Pakets durch den FTD zu ermöglichen, muss eine Regel in ACP hinzugefügt werden. Die Aktion kann entweder Zulassen oder Vertrauenswürdig sein, was vom Ziel abhängt (wenn Sie beispielsweise eine L7-Überprüfung anwenden möchten, müssen Sie Folgendes verwenden: Allow Aktion) wie im Bild gezeigt:

The screenshot shows the Cisco FTD GUI configuration page for an Access Control Policy (ACP1). The 'Rules' tab is active, displaying a table of rules. A rule named 'Rule1' is highlighted, showing its configuration details. The rule is set to allow traffic from source network 192.168.1.40 to destination network 192.168.2.40. The action is set to 'Allow'.

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

Die in der FTD Snort Engine bereitgestellte Richtlinie:

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

In LINA-Engine:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=1) 0xb788b786
```

Verhalten überprüfen

Die Paketverfolgung zeigt an, dass das Paket mit der Regel übereinstimmt. 268435460 in LINA und 268435461 in Snort-Engine:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
  This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: allow rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
...
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

Szenario 3. Vorfilter Analyse mit ACP Trust Rule

Falls der ACP eine Trust-Regel enthält, haben Sie diese, wie im Bild gezeigt:

Access Control ▸ Access Control Network Discovery Application Detectors Correlation Actions ▾

ACP1

Enter Description

Prefilter Policy: [Prefilter_Policy1](#) SSL Policy: [None](#) Identif...

Inheritance Se...

Rules Security Intelligence HTTP Responses Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rul...

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
▼ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	→ Trust
▼ Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action											Access Control: Block All Traffic		

Snort:

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

LINA:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=2) 0xb788b786
```

Beachten Sie, dass die Trust-Regel als implementiert wird, da SI standardmäßig aktiviert ist. **permit** auf LINA, sodass mindestens einige Pakete zur Überprüfung an die Snort-Engine umgeleitet werden.

Verhalten überprüfen

Packet-Tracer zeigt, dass die Snort-Engine das Paket zulässt und den Restfluss im Wesentlichen an LINA auslagert:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
```

Additional Information:

Snort Trace:

Packet: ICMP

AppID: service ICMP (3501), application unknown (0)

Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 8, icmpCode 0

Firewall: **trust/fastpath rule, id 268435461, allow**

NAP id 1, IPS id 0, **Verdict PERMITLIST**

Snort Verdict: (fast-forward) fast forward this flow

...

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

output-line-status: up

Action: allow

Szenario 4. Vorfilter Analyse mit ACP Trust Rule

In diesem Szenario wurde die SI manuell deaktiviert.

Die Regel wird in Snort wie folgt bereitgestellt:

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

In LINA wird die Regel als vertrauenswürdig bereitgestellt. Ein Paket stimmt jedoch mit der Zulässigkeitsregel überein (siehe Anzahl der ACE-Treffer), die aufgrund der Analyse Prefilter-Regel bereitgestellt wird, und das Paket wird von der Snort-Engine geprüft:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=3) 0xb788b786
...
access-list CSM_FW_ACL_ line 13 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
...
access-list CSM_FW_ACL_ line 16 advanced deny ip any any rule-id 268435458 event-log flow-start
(hitcnt=0) 0x97aa021a
```

Verhalten überprüfen

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

...

Phase: 14

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Trace:

Packet: ICMP

AppID: service ICMP (3501), application unknown (0)

Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 8, icmpCode 0

Firewall: **trust/fastpath rule, id 268435461, allow**

NAP id 1, IPS id 0, **Verdict PERMITLIST**

Snort Verdict: (fast-forward) fast forward this flow

...

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

output-line-status: up

Action: allow

Wichtigste Punkte

- Die Fehlermeldung **Analyze** Die Aktion wird als Zulässigkeitsregel in der LINA-Engine bereitgestellt. Dies wirkt sich auf das Paket aus, das zur Überprüfung an die Snort-Engine weitergeleitet wird.
- Die Fehlermeldung **Analyze** Die Aktion stellt keine Regel im Snort-Modul bereit. Daher müssen Sie sicherstellen, dass Sie eine Regel in ACP konfigurieren, die in Snort<
- Dies hängt von der ACP-Regel ab, die in der Snort-Engine bereitgestellt wird (**block** vs **allow** vs **fastpath**) keines oder alle oder einige Pakete sind von Snort erlaubt

Anwendungsbeispiele

- Ein Anwendungsfall von **Analyze** Aktion ist, wenn Sie eine umfassende Fastpath-Regel in der Prefilter-Richtlinie haben und einige Ausnahmen für bestimmte Flows festlegen möchten, sodass diese von Snort geprüft werden

AKP-Überwachungsaktion

Eine auf der FMC-Benutzeroberfläche konfigurierte Überwachungsregel:

The screenshot shows the configuration page for ACP1 in the FMC. The page includes a search bar, tabs for Rules, Security Intelligence, HTTP Responses, Logging, and Advanced. Below the tabs is a table of rules. The table has columns for Name, Source Zones, Destination Zones, Source Networks, Destination Networks, VLAN Tags, Users, Applications, Source Ports, Destination Ports, URLs, Source SGT, Destination SGT, Action, and various icons. The first rule is 'Mandatory - ACP1 (1-3)' with a sub-row for 'Monitor_Rule'.

Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Sou... Ports	Dest Ports	URLs	Sou... SGT	Dest SGT	Action	Icons
▼ Mandatory - ACP1 (1-3)														
1 Monitor_Rule	Any	Any	192.168.10.0/24	192.168.11.0/24	Any	Any	Any	Any	Any	Any	Any	Any	Monitor	Icons

Die Überwachungsregel wird auf der FTD LINA-Engine als **permit** und die Snort-Engine als **audit** aktion.

```
firepower# show access-list
```

```
...  
access-list CSM_FW_ACL_ line 10 advanced permit ip 192.168.10.0 255.255.255.0 192.168.11.0  
255.255.255.0 rule-id 268438863 (hitcnt=0) 0x61bbaf0c
```

Die Snort-Regel:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules  
...  
# Start of AC rule.  
268438863 audit any 192.168.10.0 24 any any 192.168.11.0 24 any any any (log dcfoward flowend)  
# End rule 268438863
```

Wichtigste Punkte

- Die Überwachungsregel lässt keinen Datenverkehr zu oder verwirft ihn, generiert jedoch ein Verbindungsereignis. Das Paket wird anhand nachfolgender Regeln geprüft und entweder zugelassen oder verworfen
- FMC-Verbindungsereignisse zeigen, dass das Paket zwei Regeln entspricht:

	First Packet ×	Last Packet ×	Action ×	Initiator IP ×	Responder IP ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	Access Control Policy ×	Access Control Rule ×
▼	2020-06-20 22:17:40	2020-06-20 22:17:43	Trust	192.168.10.50	192.168.11.50	41920 / tcp	80 (http) / tcp	ACP1	trust_L3-L4_Monitor_Rule

System support trace zeigt, dass Pakete beiden Regeln entsprechen:

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y  
Please specify an IP protocol: tcp  
Please specify a client IP address: 192.168.10.50  
Please specify a client port:  
Please specify a server IP address: 192.168.11.50  
Please specify a server port:  
Monitoring packet tracer and firewall debug messages
```

```
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 419031630  
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session  
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application  
unknown (0)  
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 new firewall session  
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 Starting AC with minimum 2, 'Monitor_Rule',  
and IPProto first with zone s -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source  
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0, svc 0, payload 0,  
client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
```

```
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 2, 'Monitor_Rule', action Audit
```

```
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 3, 'trust_L3-L4', action Trust
```

```
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 MidRecovery data sent for rule id: 268438858,rule_action:3, rev id:1078 02206, rule_match flag:0x2
```

Anwendungsbeispiele

Wird zum Überwachen der Netzwerkaktivität und zum Generieren eines Verbindungsereignisses verwendet

Interaktive AKP-Blockaktion

Eine interaktive Blockierungsregel, die auf der FMC-Benutzeroberfläche konfiguriert wurde:

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
▼ Mandatory - ACP1 (1-4)													
1	Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Interactive Block
2	Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Interactive Block

Die Interactive Block-Regel wird auf der FTD LINA-Engine als **permit** Aktion und zur Snort-Engine als Umgehungsregel:

```
firepower# show access-list
```

```
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=3) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Snort-Engine:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
...
# Start of AC rule.
268438864 bypass any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 bypass any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

Die interaktive Blockierungsregel fordert den Benutzer auf, das Ziel zu blockieren.

Access Denied


You are attempting to access a forbidden site.

You may continue to the site by clicking on the button below.
Note: You must have cookies enabled in your browser to continue.

Consult your system administrator for details.

Continue

Standardmäßig lässt die Firewall den Block 600 Sekunden lang umgehen:

Rules	Security Intelligence	HTTP Responses	Logging	Advanced
General Settings 				
Maximum URL characters to store in connection events				1024
Allow an Interactive Block to bypass blocking for (seconds)				600
Retry URL cache miss lookup				Yes
Enable Threat Intelligence Director				Yes
Inspect traffic during policy apply				Yes

Im **system support trace** können Sie sehen, dass die Firewall den Datenverkehr zunächst blockiert und die Blockierungsseite anzeigt:

```
> system support trace
```

```
...
```

```
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 983273680, ack 2014879580
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application unknown (0)
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 Starting AC with minimum 2, 'Inter-Block-Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589, misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 match rule order 2, 'Inter-Block-Rule1',
action Interactive
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 bypass action sending HTTP interactive response of 1093 bytes
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-Block-Rule1', drop
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions queue, drop
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 deleting firewall session flags = 0x800, fwFlags = 0x1002
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 22, NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

Sobald der Benutzer **continue** (oder aktualisiert die Browserseite) zeigt das Debugging an, dass die Pakete nach derselben Regel zulässig sind, die **Allow** aktion:

```
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1357413630, ack 2607625293
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application unknown (0)
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 Starting AC with minimum 2, 'Inter-Block-Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589, misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 match rule order 2, 'Inter-Block-Rule1', action Interactive
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 bypass action interactive bypass
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 allow action
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 8, NAP id 1, IPS id 0, Verdict PASS
```

Anwendungsbeispiele

Eine Warnseite für Webbenutzer anzeigen und ihnen die Möglichkeit geben, fortzufahren.

Interaktiver AKP-Block mit Rücksetzaktion

Ein interaktiver Block mit auf der FMC-Benutzeroberfläche konfigurierter Rücksetzregel:

Name	Sour... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Appli...	Sour... Ports	Dest Ports	URLs	Sour... SGT	Dest SGT	Action
▼ Mandatory - ACP1 (1-4)													
1	Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block with reset
2	Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Interactive Block with reset

Der Interactive Block mit der Reset-Regel wird auf der FTD LINA-Engine als **permit** Aktion und Snort-Engine als Intersect-Regel:

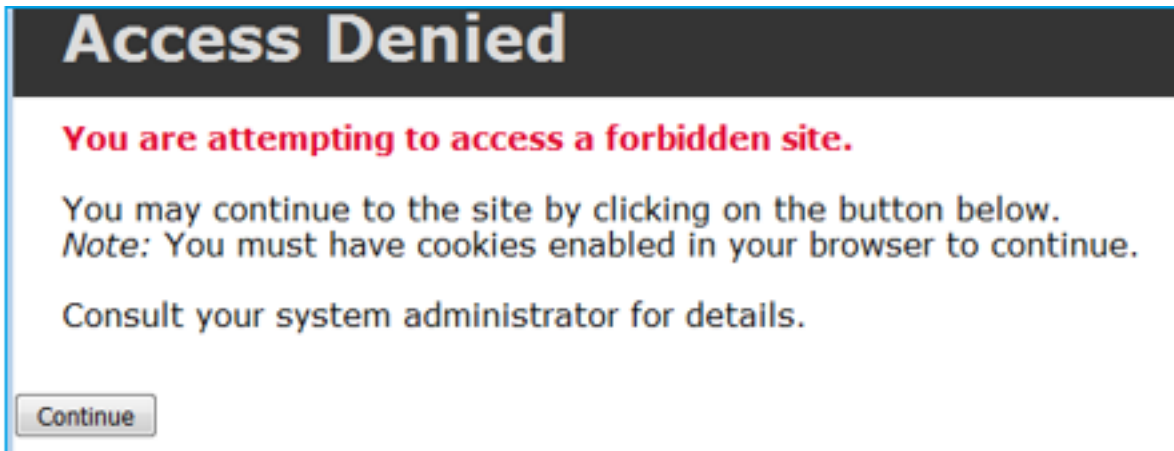
```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=13) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Snort-Engine:

```
# Start of AC rule.
268438864 interset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
```

```
# End rule 268438864
268438865 intreset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

Wie bei Block mit Zurücksetzen kann der Benutzer die **Continue** Option:



Im Snort debuggen Sie die unter Interactive Reset:

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.52
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages
```

```
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3232128039
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 new firewall session
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0, svc 0, payload 0, client 0,
misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 MidRecovery data sent for rule id:
268438864,rule_action:8, rev id:1099034206, rule_match flag:0x0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 HitCount data sent for rule id: 268438864,
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2228213518, ack
3232128040
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
```

```
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 bypass action sending HTTP interactive
response of 1093 bytes
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-
Block-Rule1', drop
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
BLACKLIST
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

An dieser Stelle wird dem Endbenutzer die Blockseite angezeigt. Wenn der Benutzer **continue** (oder aktualisiert die Webseite) die gleiche Regel erfüllt, die den Datenverkehr diesmal zulässt durch:

```
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1593478294, ack
3135589307
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 bypass action interactive bypass
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 allow action
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3135589307, ack
1593478786
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS
```

Der interaktive Block mit Reset-Regel sendet eine TCP-RST an Datenverkehr, der nicht zum Web gehört:

```
firepower# show cap CAPI | i 11.50
 2: 22:13:33.112954      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: S
3109534920:3109534920(0) win 29200 <mss 1460,sackOK,timestamp 3745225378 0,nop,wscale 7>
 3: 22:13:33.113626      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: S
3422362500:3422362500(0) ack 3109534921 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
53252448 3745225378>
 4: 22:13:33.113824      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362501 win 229 <nop,nop,timestamp 3745225379 53252448>
 5: 22:13:33.114953      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362501:3422362543(42) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 6: 22:13:33.114984      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362543:3422362549(6) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 7: 22:13:33.114984      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362549:3422362570(21) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 8: 22:13:33.115182      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362543 win 229 <nop,nop,timestamp 3745225381 53252448>
 9: 22:13:33.115411      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362549 win 229 <nop,nop,timestamp 3745225381 53252448>
10: 22:13:33.115426      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362570 win 229 <nop,nop,timestamp 3745225381 53252448>
12: 22:13:34.803699      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: P
3109534921:3109534931(10) ack 3422362570 win 229 <nop,nop,timestamp 3745227069 53252448>
13: 22:13:34.804523      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: R
3422362570:3422362570(0) ack 3109534931 win 0
```

Sekundäre FTD-Verbindungen und Pinholes

In älteren Versionen (z. B. 6.2.2, 6.2.3 usw.) öffnet die Snort-Engine keine Pinholes für sekundäre Verbindungen (z. B. FTD-Daten), wenn Sie die `trust` aktion. In den letzten Versionen wurde dieses Verhalten geändert, und die Snort-Engine öffnet Pinholes sogar mit dem `Trust` aktion.

FTD-Richtlinien

- Verwenden Sie Fastpath-Vorfilterrichtlinien für große Fettflüsse und zur Verringerung der Latenz durch das Gerät.
- Verwenden Sie Vorfilter-Blockierungsregeln für Datenverkehr, der basierend auf L3/L4-Bedingungen blockiert werden muss.
- Verwenden Sie ACP Trust-Regeln, wenn Sie viele der Snort-Prüfungen umgehen, aber dennoch Funktionen wie Identitätsrichtlinie, QoS, SI, Anwendungserkennung und URL-Filter nutzen möchten.
- Legen Sie mithilfe der folgenden Richtlinien Regeln, die sich weniger auf die Firewall-Leistung auswirken, an die Spitze der Zugriffskontrollrichtlinie:

1. Sperrregeln (Layer 1-4) - Vorfilter Block
2. Regeln zulassen (Layer 1-4) - FastPath vorfiltern
3. ACP-Blockregeln (Layer 1-4)
4. Vertrauenswürdige Regeln (Layer 1-4)
5. Blockierungsregeln (Layer 5-7 - Anwendungserkennung, URL-Filterung)
6. Zulassen von Regeln (Layer 1-7 - Anwendungserkennung, URL-Filterung, Angriffsrichtlinie/Datei richtlinie)

7. Regel sperren (Standardregel)

- Vermeidung übermäßiger Protokollierung (am Anfang oder am Ende protokollieren und beides gleichzeitig vermeiden)
- Achten Sie auf die Regelerweiterung, um die Anzahl der Regeln in LINA zu überprüfen.

```
firepower# show access-list | include elements
access-list CSM_FW_ACL; 7 elements; name hash: 0x4a69e3f3
```

Zusammenfassung

Vorfilteraktionen

Rule Action (FMC UI)	LINA Action	Snort Action	Notes
Fastpath	Trust	Fastpath	Static Flow Offload to SmartNIC (4100/9300). No packets are sent to Snort engine.
Analyze	Permit	-	The ACP rules are checked. Few or all packets are sent to Snort engine for inspection. Traffic is allowed or dropped based on Snort engine verdict
Block (Prefilter)	Deny	-	Early drop by FTD LINA No packets are sent to Snort engine

AKP-Aktionen

Rule Action (FMC UI)	Additional Conditions	LINA Action	Snort Action	Notes
Block	The rule matches L3/L4 conditions	Deny	Deny	
Block	The rule has L7 conditions	Permit	Deny	
Allow		Permit	Allow	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, or ID) enabled	Permit	Fastpath	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, and ID) disabled	Trust	Fastpath	Static Flow Offload (4100/9300)
Monitor		Permit	Audit	Monitor Rule doesn't drop or permit traffic, but it generates a Connection Event. The packet is checked against subsequent rules and it is either allowed or dropped
Block with reset		Permit	Reset	When a packet matches Block with reset rule FTD sends a TCP Reset packet or an ICMP Type 3 Code 13 Destination Unreachable (Administratively filtered) message
Interactive Block		Permit	Bypass	Interactive Block Rule prompts the user that the destination is forbidden If bypassed, by default, the firewall allows to bypass the block for 600 seconds
Interactive Block with reset		Permit	Intreset	Same as Interactive Block with the addition of a TCP RST in case of non-web traffic

Anmerkung: Ab 6.3 FTD-Softwarecode kann Dynamic Flow Offload Verbindungen auslagern, die zusätzliche Kriterien erfüllen, z. B. vertrauenswürdige Pakete, die eine Snort-Prüfung erfordern. Weitere Informationen finden Sie im Abschnitt "Offload Large Connections (Flows)" im Konfigurationsleitfaden für das FirePOWER Management Center

Zugehörige Informationen

- [FTD-Zugriffskontrollregeln](#)
- [FTD-Vorfilter- und Vorfilterrichtlinien](#)
- [Analyse der FirePOWER-Firewall-Erfassung zur effektiven Behebung von Netzwerkproblemen](#)
- [Arbeiten mit Firepower Threat Defense \(FTD\)-Erfassungen und Packet-Tracer](#)
- [Konfigurieren der Anmeldung bei FTD über FMC](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)
- [Große Verbindungen auslagern](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.